ElectioNet™

State of New Jersey Office of the Attorney General Division of Elections

Documentation of Hosting Infrastructure for the Statewide Voter Registration System (SVRS)

NEW JERSEY

Deliverable SVRS 100

Presented to:
Michael Gallagher
SVRS Project Manager
Department of Law and Public Safety
Trenton, New Jersey

Presented by:
Covansys Corporation
32605 West 12 Mile Road
Farmington Hills, MI 48334

June 2005

Revision History

Date	Brief Description	Changed By:
06/14/2005	Initial Draft	Wm. Gary Bush
06/23/2005	Version 1	Chad Duling

Table of Contents

1.0 DOCUMENTATION OF THE HOSTING INFRASTRUCTURE

The foundation of our hosting service is to ensure that your application is always available and is constantly operating at peak performance levels.

Covansys offers a suite of Service Level Agreement (SLA) offerings to our hosting customers. Covansys' SLA offerings are designed to make servers available as close to 100% of the time as possible.

Through both standard and custom SLA offerings, Covansys can provide clients with proactive management of the performance and availability of mission-critical applications and web servers.

To achieve a 98.5% SLA, Covansys has designed a redundant configuration with no single points of failure. All critical hosting components are addressed, including:

- Self Healing Mesh Network Design
- 24-7 Monitoring and Support
- Advanced Reporting capabilities
- Security Assessment Services
- Standardized and customizable escalation and notification procedures
- Redundant electrical and cooling systems, with full generator backup

SLA Offerings

As an organization, SLA offerings provide you with guarantees and proactive management of the performance and availability of your applications and services. In addition to our standard SLA offering, Covansys can develop customized agreements for extraordinary cases and more complex configurations.

Covansys Standard Service Level Agreement (SLA)

- 95% availability for each managed non-redundant server
- 98.5% availability for managed high-availability configurations

With the Covansys SLA, you receive comprehensive coverage for the entire infrastructure, including the data centers, network, servers, equipment and operational processes. Our process flow is designed so that your application will be operating as close to 24x7x365 as possible. We reinforce this commitment by having dedicated offshore support personnel who are available 24 hours a day, seven days a week. We also have on-site expert engineers with technical certifications from leading companies such as Microsoft, Sun and Cisco.

Middletown Data Center Architecture

The Covansys Middletown Data Center has its own dedicated support systems, including multiple communications feeds, independently monitored and metered electrical control units, as well as generator backed uninterruptible power supplies (UPS).

The computer room is completely independent from the rest of the facility, ensuring that problems remain isolated and that potentially disastrous situations remain contained.

The entrance to the computer room is through highly secured entryways, protected with Sonitrol Access Card control systems, providing protection against unlawful entry. Third party vendors and technicians must be escorted to enter the Data Center and the escorts stay with them the entire time.

Environmental Controls

The Middletown environmental systems have been designed to provide for optimum temperature and humidity controls in the computer room, at all times. Equipment heat output and power consumption are closely monitored, and capacity planning insures that cooling units and electrical systems have enough overhead at all times.

Air Conditioning – Computer room environmental parameters are controlled by three redundant computer room air conditioners. These units are generator backed, providing environmental controls even in the event of power failure.

Heat Capacity Management – Covansys data center personnel closely monitor and manage the BTU output of all servers and equipment in the data center, ensuring that cooling capacities are never overtaxed.

Power

The Data Center was designed with the latest power-protection technology to keep your application infrastructure in continuous operation.

Uninterruptible Power Supply (UPS) – Covansys has installed four redundant UPS systems to handle any short-term loss of utility power. These UPS systems also ensure the smooth and seamless transfer from utility to generator power. Furthermore, the UPS system has been designed to allow for additional expansion, when required.

Generators – Covansys has installed Generators at each facility in the event that utility power is unavailable for an extended period. These systems use natural gas, ensuring that fuel supplies are constant and virtually uninterruptible.

Details of Data Center Electrical and Wiring Construction
Electrical Configuration
Data Center power is available at standard 110v or 208v or 240v for AS/400, Servers, and other special needs
All data center power is supplied through enterprise class UPS units – servers and equipment are assured a clean sine wave at the proper voltage – eliminating surge and brownout risks
Power consumption is closely monitored and managed in each server rack, ensuring that servers are

Details of Data Center Electrical and Wiring Construction
never affected by overloading,
Data center power is backed by natural gas generators capable of sustaining all hosted environments, network equipment, and HVAC equipment throughout an outage of any duration
Electrical Room Segregation
Electrical panels, transformers, and UPS controllers and batteries are all segregated.
Machine rooms are HVAC controlled.
Cable and Patch Management
Data center network cabling runs on wire trays suspended above the server racks, eliminating the mess and confusion often caused by masses of cabling underneath a raised floor
Wire trays, combined with color coding and strict labeling policies ensure that environments can be quickly re-patched and rerouted in the event of an emergency

Physical Security

Access to Covansys server facilities are restricted to Data Center employees only, all outside personnel are accompanied by Data Center representatives at all times. Access requires passing multiple levels of keycard access. Access to this facility is strictly limited to those persons wishing to gain access to their machines or evaluating the facility for future business. Such persons are continuously escorted while on premises, effectively preventing physical attempts to gain unauthorized access.

Parameter driven Card-Key access ensures that even Covansys staff members are limited in access to only those areas for which they have been approved, and nothing more.

Details of Physical Security
Four-level security architecture
Card-Key access to Level 0 (includes lobby and public areas)
Card-Key plus Level 1 (Office and Support Environments)
Card-Key (restricted) to pass from Level 1 to Level 2
Card-Key (restricted to Server Admin Personnel) to access Level 3 (Standard Server Rooms)
Data Center facility is fully alarmed, with automated fire and police notification and response

Electronic Security

Additional levels of role-based security are applied to the monitoring and administration backbone network, including heightened access restrictions, increased intrusion detection, and proactive real-time server monitoring. Only authorized Data Center personnel with tightly monitored administrative privileges have any access to the network. In addition, access to the tape backup system is limited to authorized personnel, and is physically restricted to certain machines and network segments.

Fire Suppression

Covansys fire suppression systems provide advanced fire protection.

Details of Fire Protection
Multiple sensors located throughout the buildings to test and pinpoint the source of trouble
Independent Inergen based non-conductive, non-corrosive gaseous fire suppression system prevents damage to the equipment, with incipient-phase early-warning primary smoke detection

Computer Rooms: Fire Suppression

The computer room has an independent gaseous fire suppression system with incipient-phase early-warning primary smoke detection capabilities. This system requires that two detectors identify a fire situation. This prevents false triggers from fan burnouts and other minor hardware failures.

Once the building alarm systems are activated, security and local fire authorities are notified. A short delay allows staff to evacuate the computer room prior to system activation. A non-conductive and non-corrosive gas is then released into the room to extinguish the fire.

The Network

Covansys networking services are designed to ensure that your application is always operational and always available. Our network strategy was designed to provide customers with superior levels of throughput and reliability, while maximizing efficiency and eliminating single points of failure. We have multiple partnerships with the industry leading network providers in AT&T, WorldCom, and Broadwing to provide global networking services. The Covansys internal data center network is designed with fault tolerance in mind and with no single points of failure. Covansys can provide services such as session based traffic balancing, geographical distribution of network traffic and burstable bandwidth to ensure that your Web site receives the highest levels of availability.

Internet Connectivity

Covansys combines leading telecommunications technology partnerships with the latest hardware and software to provide you with exceptional Internet connectivity. Covansys offers networking services through a DS3 based Internet backbone.

Covansys partners with AT&T as our primary provider of network services, ensuring that we have direct access to one of the fastest and most reliable Internet backbones in the industry. Over 50% of all Internet traffic goes across the AT&T backbone. By having your Web site directly connected to the AT&T backbone, you can be assured that you are receiving reliable Internet access.

AT&T's network maintains high levels of reliability with redundant, diverse paths to avoid single points of failure and provide optimal routing and traffic flow, as well as uninterruptible power supplies at every switching node. The backbone is a pure IP-routed network that segments into other services such as voice or fax, so your data never has to share bandwidth with non-IP traffic.

AT&T's multi-tiered architecture provides extra protection since performance problems in one region do not create disasters for other regions

Details of AT&T Network
Connected to the Covansys Data Centers through DS3 and Multiple T1 circuits
Spans over 2,500+ worldwide points of presence (POPs)
Provides connectivity in 100+ countries on 5 continents
Incorporates 1.6 million modem ports Best-of-class availability and reliability

Covansys Data Center Network

The Covansys Data Center network, a Cisco-powered network, is designed for the utmost in scalability and built-in redundancy. The data center network features fully redundant routers, redundant switching and redundant connections to eliminate failure points within the data center. This strategy ensures our clients that Covansys backbone performance is as fast and as reliable as possible.

Details of Data Center Network Infrastructure
Connected to the AT&T and Level 3 network through multiple DS3 circuits
Redundant Cisco routers, each of which is connected to generator backed redundant Uninterruptible Power Supplies (UPS)
Multiple network connections to the Internet, providing a back-up path for traffic, ensuring continuous access to your site
A totally separate back-up network, so archiving data and other maintenance procedures can occur at the same time as site transactions, with no lapse in performance

Expansion and Bandwidth

Covansys strategy for the expansion of the network is to allow no more than 60% utilization on any given segment. When utilization exceeds this threshold, we work with providers to upgrade the routers and circuits. Covansys is focused on expanding our global services through relationships with global Telco and Internet service providers. These strategies continue to ensure our clients that Covansys networking services are as fast and as reliable as possible.

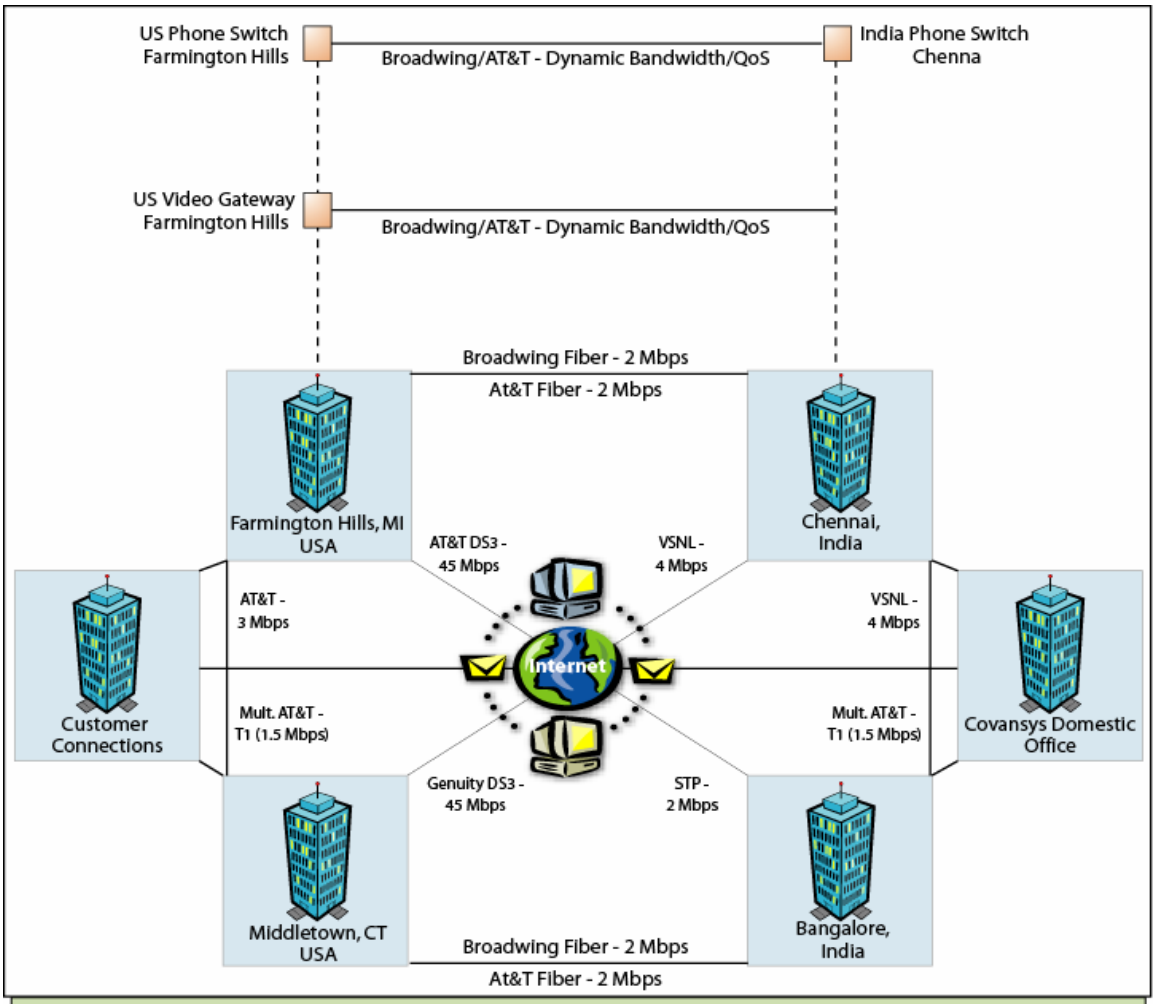
Covansys offers burst able Internet bandwidth. The combination of a Committed Information Rate (CIR) and an Available Information Rate (AIR) gives you flexibility and assured reliability. For example, you may not need a full 5Mbps of throughput 24 hours per day, seven days a week. However, a short-term event may cause traffic to increase substantially for a week's period, then return to normal. In this case, you would have a committed information rate of 1Mbps with an AIR of 5Mbps in order to compensate for the high burst in traffic.

The benefit to you is that you pay only for the amount of bandwidth that you actually utilize while having the peace of mind that additional bandwidth is available. Bandwidth can be increased or decreased with reasonable advance notice.

Network Connectivity and Architecture Services

This section outlines the services that will be provided by Covansys in the Client Network Technology Architecture Services area.

Current Network Infrastructure



Redundancy and Failover

Farmington Hills
- AT&T 3Mbps (FTH to Chennai)
- Broadwing 2Mbs (FTH to Chennai)
- AT&T DS-3 (Internet)
- AT&T 3Mbs (FTH to Middletown)
- AT&T 1.5Mbs (FTH to Offices)

Middletown, CT
- AT&T 2Mbs (Middletown to Bangalore)
- Broadwing 2Mbs (Middletown to Bangalore)
- Genuity DS-3 (Internet)

Chennai, India
- AT&T 2 Mbs (FTH to Chennai)
- Sprint 3Mbs (FTH to Chennai)
- VSNL 2Mbs (Internet)
- VSNL 4Mbs (Chennai to Bangalore)

Bangalore, India
- AT&T 2Mbs (Middletown to Bangalore)
- STP 2Mbs (Internet)
- VSNL 4Mbs (Chennai to Bangalore)

8Mbs of Fiber bandwidth to India (Voice, Video & Data)
4Mbs Internet bandwidth in India
100Mbs Internet bandwidth in U.S.

Figure 1. Network Infrastructure

In addition to our existing network capacity we will be adding a T3 45Mbps AT&T MPLS circuit. This circuit will be dedicated for the usage of the New Jersey SVRS system. This will be the circuit used for both county replication as well as direct end user access.

Security

Covansys security offerings ensure that your corporate assets and e-business processes are tightly secured and protected at all times. State-of-the-art security is built into every aspect of Covansys managed hosting solutions. Our industry-leading protections range from physical and internal security, to operating system and network security.

Covansys Security Solutions work for you to:

- Protect your assets with the latest, tested security products, tools and techniques.
- Proactively identify potential vulnerabilities and exposures that can threaten to take down your business and cost you valuable transaction processing.
- "Lock down" your Web servers by constantly monitoring security updates from vendors and industry associations and applying upgrades and patches on a regular basis.
- Provide secured and encrypted methods to exchange sensitive and confidential data in an economical way over the Internet.
- Meet physical security needs, including video surveillance, keycard entry, motion detection and other state of the art technologies.

Covansys Security Team

Covansys has a dedicated Security team, responsible for identification, monitoring, and mitigating security threats. The security team performs policy definition and works integrally with other Covansys organizations to enforce security policies. The Security resources are composed of information security experts, dedicated server administrators, and network personnel who work together to achieve optimum security at the network, system and physical access levels. This team monitors industry security information sources and underground communities for late-breaking security threats.

In addition, best practices are recommended and enforced by the Security team. By defining policies for internal access to servers, facilities and other corporate resources, the security team ensures that there are no gray areas where oversights can occur.

Data and Access Security

To provide an additional level of security, Covansys ensures that all system management is performed over a secure back-end network. Only authorized personnel with administrative privileges have access to the network. Customer connections to network switches are accomplished via Layer 2 Virtual Local Area Networks (VLANs), which logically segregate all customer traffic. This prevents data "sniffing" within the data center, and prevents attackers and viruses from 'leapfrogging' from one environment to another in the event of a security breach.

Server/Software Security

Covansys data center administrators continually monitor every managed server hosted within the data centers, ensuring that the most recent security patches and fixes have been installed. As soon as your site or application environment is established, Covansys engineers and the Security team utilize a unique and thorough "lock-down" approach. This procedure disables unnecessary user IDs, closes down known hacker back doors and removes processes that are not required, such as e-mail services.

Once the server is migrated into production, the Covansys security team monitors vendor security updates, hacker sites and security industry sites to understand where there may be possible exposures.

One of the cornerstones of the Covansys server security architecture is the hardened server-build process. Risk-prone services are "locked down" to minimize the chance of security exposures. The following provides details on our secure, proprietary server-build process:

Standardization – Covansys is able to offer higher levels of security through standardization. Covansys staffs a dedicated team of engineers responsible for updating, optimizing and securing the Covansys standard build. The build process is fully standardized and repeatable. Repeatability ensures that each of your Covansys servers has the same secure version of the operating system and Web server software.

Secure Build – The standard build is regularly updated with the latest security patches. Risk-prone services such as netBIOS and SMTP are "locked down" to mitigate security exploits. Security features include encryption services through PPTP, IPSec, SSL and Kerberos authentication, combined with Covansys' rapid notification and response to security threats.

In addition, several secure remote administration tools are available for encrypted connections to your server:

Terminal Server Remote Administration – Point-to-Point Tunneling Protocol (PPTP) is recommended for administrators to perform secure, remote administration of your Covansys server. PPTP creates private "tunnels" across the public Internet over which secure communications can be sent.

UNIX Remote Administration – Secure Shell (SSH) is recommended for UNIX administrators to perform secure, remote administration of your Covansys server. SSH is recommended as a secure alternative to rcp, rsh, rlogin and telnet.

Network Security

Covansys network architecture ensures that all of your data—within and outside of Covansys—is protected at all times through heightened levels of security and stringent security policies that are applied to the back-end network. Only authorized personnel with administrative privileges have access to the network as well as the tape backup system..

We offer the following measures to provide the most stringent network protection:

Kerberos Authentication – Covansys uses Kerberos to ensure secure communication between servers within the data center network. Kerberos mitigates the risk of compromise due to hacker programs such as sniffers. A sniffer program is designed to listen to network traffic for useful information such as passwords and logins. Kerberos encrypts traffic sent between servers on the Covansys data center LAN to minimize risks. It also provides trusted third party authentication of the sender's identity and keeps an audit trail of login attempts.

Secure Back-End Administration Network – Covansys uses a proprietary, back-end network to backup and monitor servers through secure connections. With our non-routable network, you are assured that external parties cannot directly contact the IP addresses of these servers.

Network Segmentation – Customer server clusters are located on many different network segments. Hacker sniffer programs can usually only listen in on traffic on a particular network segment. Through the use of Kerberos and network segmentation, the spread of intruders is minimized and it is difficult to jump from one segment to another segment of the network.

Network Level Segregation is achieved as follows:

- We will implement a separate VLAN (Virtual LAN) for our Customers
- Within the overall Customer VLAN Network, we can isolate a particular program/application using only Layer 2 switching configuration.
- Traffic can be routed via a firewall interface to the rest of the VLAN.
- We can secure this Network using DMZ configuration.
- Access will be permitted only to client workstation belonging to the Customer VLAN.
- VMPS – VLAN Management Policy Server
- We use MAC address based VLAN mapping using VLAN Management Policy Server to achieve higher security.